Forrester-Report: Unzureichende unternehmensweite Kollaboration erschwert Management des externen Cyber-Risikos
Größte Herausforderungen sind unzureichende Kommunikation, heterogene Tool-Landschaft und unklare Zuständigkeiten --- Einheitliche Tools für gezielte Automatisierung und Single Source of Truth sind effektivste Gegenmaßnahmen

PALO ALTO, 3. August 2023 --- Die Ansprüche an ein effektives Risikomanagement der externen Angriffsfläche, die ein Unternehmen über aus dem Internet erreichbare IT-Assets bietet, und die reale Situation klaffen in Unternehmen weit auseinander. Zu diesem Schluss kommt ein vom Analystenhaus Forrester erstellter Thought Leadership Report, der von CyCognito, Marktführer für External Attack Surface Risk Management (EASM), in Auftrag gegeben wurde. Dafür wurden insgesamt 304 Security- und IT-Entscheider in den USA, Deutschland, Frankreich, Großbritannien und Kanada befragt, die unternehmensintern auch für die Risikobewertung verantwortlich sind.

Größte Hürden für ein effektives Management sind demnach unzureichende Kommunikation, eine heterogene Tool-Landschaft, unklare Zuständigkeiten sowie ineffektive Methoden zur Priorisierung von Risiken - und damit vor allem Herausforderungen im Hinblick auf eine funktionierende Kollaboration. Abhilfe schaffen zentral genutzte Tools für eine rasche Erkennung (Mean Time to Detection - MTTD), die eine schnellere durchschnittliche Behebungszeiten (MTTR) ermöglichen, und eine Single Source of Truth als einheitliche Informationsgrundlage.

Tool-Wildwuchs und mangelnde Kollaboration erhöhen Risiko

Unentdeckte Sicherheitslücken in über das Internet erreichbaren Assets, beispielsweise unsicher konfigurierte Cloud-Lösungen, Datenbanken, IoT-Devices und Co., bergen ein enormes Risiko für die IT-Sicherheit von Unternehmen. Gleichzeitig entsprechen aktuelle Risikomanagementpraktiken für das Identifizieren, Priorisieren und Beheben dieser Schwachstellen selten den Erwartungen der Verantwortlichen. Obwohl 81 Prozent der Befragten Sicherheitstests, -prozesse oder -übungen zur Aufdeckung von Schwachstellen in Sicherheitskontrollen und -mechanismen als wichtiges Instrument des Risikomanagements einstufen, wurden bei 53 Prozent im Zuge der letzten Risikobewertung eine beträchtliche Anzahl unentdeckter externer Assets gefunden.

Diese Diskrepanz liegt gemäß Forrester vor allem an unzureichender interner Zusammenarbeit - ein Umstand, der sich anhand mehrerer Ergebnisse zeigt. Ein Indikator ist die Heterogenität der Tool-Landschaft: Fast 40 Prozent der teilnehmenden Unternehmen nutzen mehr als zehn verschiedene Tools, die sich über mehrere Teams verteilen und unabhängig voneinander zum Einsatz kommen, statt die Erkenntnisse allen Beteiligten zur Verfügung zu stellen. Diese "Silos" erschweren die nötige Kommunikation und Kollaboration. Nur 22 Prozent der Befragten haben ein bereichsübergreifendes Team, das für eine effektive Priorisierung von Gegenmaßnahmen zuständig ist. Das führt dazu, dass es in einem von vier befragten Unternehmen mehrere Wochen oder sogar länger dauert, auf neue, mitunter hohe Risiken zu reagieren. Generell bewerten 40 Prozent der Befragten die Beziehungen der involvierten Teams für Security, IT und Business untereinander als durchgängig negativ.

Zentrale Automatisierungstools und Single Source of Truth schaffen Abhilfe

Um das Risiko von Sicherheitslücken in externen Assets durch eine schnelle Erkennung, Priorisierung und Behebung effektiv senken zu können, sollten Unternehmen laut dem Report zwei Maßnahmen ergreifen. Erstens sollte für das Erfassen und die Bewertung von Risiken eine unternehmensweite Single Source of Truth existieren, also eine einzige Informationsquelle, die von allen Beteiligten genutzt und permanent auf dem neuesten Stand gehalten wird. Die dafür nötige Zusammenarbeit verbessert außerdem die Stimmung zwischen den Teams und hat auch einen direkten Einfluss auf die MTTR.

Erleichtert wird dieses Ziel durch eine zweite empfohlene Maßnahme: Die Einführung einer zentralen Lösung für die Risikominderung, die wichtige Kernaufgaben automatisiert und kontinuierlich durchführt. Dazu gehört das durchgängige Abbilden von Geschäftsstrukturen, regelmäßige Sicherheitstests, die auch "blinde Flecken" finden, und das korrekte Zuordnen von Assets. Diese Maßnahmen erlauben eine einheitliche Betrachtung der externen Angriffsfläche, eine Priorisierung und Planung von Gegenmaßnahmen - und damit ein effektives Risikomanagement.

Der gesamte Report kann unter diesem Link kostenlos heruntergeladen werden.

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Axel Schreiber
Karlstraße 42
80333 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

CyCognito

Herr Dr. Georg Hess
Karlstraße 42
80333 München

https://cycognito.com
CyCognito@haffapartner.de

Über CyCognito
CyCognito ist Marktführer bei External Attack Surface Risk Management und zählt viele Fortune-2000-Unternehmen zu seinen Kunden. Von der CyCognito-Plattform profitieren aber nicht nur große Unternehmen und Konzerne, sondern auch der Mittelstand. Die Plattform erlaubt ein proaktives, kontinuierliches Management der potenziellen Angriffsfläche, die ein Unternehmen über seine mit dem Internet verbundenen Assets bietet, und hilft, die damit verbundenen Risiken zu steuern und zu minimieren.

Kontinuierliches Monitoring inklusive einem weitreichendem automatisiertem Security Testing - ohne Input seitens des Kunden - zeigt regelmäßig die jeweils vollständige Angriffsfläche einschließlich "blinder Flecken" auf. Dazu gehören beispielsweise vergessene Cloud-Assets und nicht mehr genutzte oder fehlerhaft konfigurierte IT/IoT-Infrastrukturen. Das ist jedoch nicht alles: Dank relevanter Priorisierung und umfassender Integration in bestehende Security-Prozesse und -Plattformen (SOC, SIEM, SOAR, Ticketing-Systeme) können Unternehmen mit CyCognito effektiv jeweils die zehn Security-Lücken schließen, die 90 Prozent des gesamten externen Cyber-Risikos ausmachen.

Der Hauptsitz des Unternehmens ist heute in Palo Alto. Ursprünglich stammt CyCognito aus Israel, wo sich unter anderem die R&D-Abteilung befindet.

https//www.cycognito.com

Anlage: Bild